

## REMARKS

Claims 1, 2, 6, 16, 17, 21, 22, 31, 32, 35, 36 and 41-44 are rejected under 35 U.S.C. 112, second paragraph, for the reasons of record. In making the rejection the Examiner takes issue with the recited word "trusted" saying it renders the claims indefinite. The Examiner continues by saying that "trusted" is not defined by the claim, that the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The Examiner continues by saying that "Trusted software" could be "interpreted as compatible software or executable software."

The Examiner's rejection is respectfully disagreed with and is traversed below.

First, the undersigned is not aware of a requirement that a term be defined within a claim.

Second, the phrase "trusted software" is a term of art that would be readily understood by one of ordinary skill. As an example, a check of the USPTO database finds approximately 140 U.S. Patents that have issued prior to the filing date of this application wherein the phrase "trusted software" appears at least once. Note, by example, the attached copy of U.S. 6,105,132 where "trusted software" is claimed in claims 10 and 26, and is mentioned once in the specification at col. 5, lines 39-43. Further, the term "trusted software" is defined no later than 02/28/2001 in Telecom Glossary 2K ([www.atis.org](http://www.atis.org)), as shown in the two attached pages.

Further, the phrases "trusted relationship", "trusted software" and "trusted units of code" are found throughout the specification, such as at page 4, lines 4, 5, 9 and 29; page 6, lines 18-20; page 7, line 29 to page 8, line 1; page 11, lines 13, 14 and 25-27; page 12, line 13 and in claims 2 and 17 as filed. Reference can also be made to Figures 2 and 3 for showing the TS<sub>O</sub> 11A and TS<sub>B</sub> 11B.

Clearly, the use of the term "trusted software" in the claims does not render them indefinite.

However, it is proposed to make a merely clarifying amendment to the claims above. Specifically, the claims are amended to revise all occurrences of the phrase "trusted service provisioning relationship" to read "service provisioning relationship" (as originally filed). In addition, and by example, claim 1 is amended to include some of the subject matter of claim 2, i.e., to recite "where at least establishing and recording use trusted software comprising a certified unit of code running on the user device and on the bridging user device", where support for the phrase "certified unit of code" is found in the specification at least at page 6, lines 19-21. No new matter is added. In addition, claim 16 is amended to incorporate the subject matter of claim 17, which is cancelled without prejudice or disclaimer, and a somewhat similar amendment was made to independent claims 31, 35, 41 and 43. No new matter is added.

The entry of these clarifying amendments is respectfully requested at least for the reason that no additional searching will be required on the part of the Examiner in that the subject matter of "trusted software" was found in the claims as filed.

The Examiner is respectfully requested to reconsider and remove the rejection under 35 U.S.C. 112, second paragraph.

Claims 1, 3-9, 16, 19-24, 31-38 and 41-44 are once again rejected under 35 U.S.C. 102(e) as being anticipated by US 2003/0054796 A1 (Tamaki et al.), claims 2, 17, 10, 11, 25, 26, 39 and 40 are once again rejected under 35 U.S.C. 103(a) as being unpatentable over Tamaki et al. in view of US 2004/0142686 A1 (Kirkup et al.), claims 12, 13, 27 and 28 are once again rejected under 35 U.S.C. 103(a) as being unpatentable over Tamaki et al. in view of JP 2002209028 A (Sakakura), claims 14 and 19 are once more rejected under 35 U.S.C. 103(a) as being unpatentable over Tamaki et al. in view of Sakakura, and further in view of US 2003/0061358 A1 (Piazza et al.), and claims 15 and 30 are again rejected under 35 U.S.C. 103(a) as being unpatentable over Tamaki et al. in view of Sakakura, and further in view of US 2004/0117358 A1 (VonKaenel et al.) These rejections are respectfully disagreed with, and are traversed below.

In rejecting claims 2, 17, 10, 11, 25, 26, 39 and 40 under 35 U.S.C. 103(a) as being unpatentable

over Tamaki et al. in view of Kirkup et al. the Examiner once again acknowledges that Tamaki et al. do not teach the use of trusted software, but then states that this limitation is taught by Kirkup et al. in paragraph [0084]. The Examiner then further states that it would have been obvious to apply the teachings of Kirkup et al. to Tamaki et al. in order to "provide security for users and for the network".

It is once more respectfully pointed out that what Kirkup et al. disclose in paragraph [0084] is the following:

[0084] It is also contemplated that **certain trusted software applications could be permitted to open both internal and external connections on a mobile device**. A software application provided by an owner of the mobile device, for example, is generally trusted by the owner and might be allowed both internal and external connections. This may be accomplished in a connection policy store with an entry of the form shown in FIG. 2 for application C, for example, or an authorization record store where authorization records are used. All software applications provided by a mobile device owner or sources trusted by the owner, or only software applications identified in a trusted application list stored on the mobile device, could be permitted to open both types of connections. (emphasis added)

That is, the disclosure of Kirkup et al. is in the context of using a user-provided or other-provided trusted software application within a given mobile device to selectively control access to internal and external connections. However, claim 2 of the instant patent application refers to trusted software used at least in the establishing operation of claim 1, that is claimed as:

**"establishing a service provisioning relationship between the user device and a bridging user device through a first wireless network"** (emphasis added).

Clearly, any use of a trusted software application in Kirkup et al. to simply permit opening both internal and external connections on the mobile device does not suggest such use in "establishing a service provisioning relationship between the user device and a bridging user device" as in claim 1.

The amendment that was discussed above to the independent claims should serve to clearly distinguish the independent claims from the proposed combination of Tamaki et al. and Kirkup et al.

As was noted above, and by example, claim 1 now recites in part:

"where at least establishing and recording use trusted software comprising a certified unit of code running on the user device and on the bridging user device."

In that the Examiner acknowledges that Tamaki et al. do not teach the use of trusted software, and in that it has been shown that Kirkup et al. use a trusted software application for simply enabling the selective control of access to internal and external connections of a given mobile device, the resulting amended independent claims should all be found to be allowable, and to be in condition for allowance. That is, even if the "trusted software applications" of Kirkup et al. were incorporated into at least one of the end user terminals 111-114 and into the personal communications providers terminals 115-117 of Tamaki et al., which is not admitted is suggested, the resulting modified terminals would appear at best to simply "be permitted to open both internal and external connections". There is no suggestion in such a proposed modification that there would be executed, e.g., as in amended claim 1, establishing a service provisioning relationship between a user device and a bridging user device through a first wireless network, providing a desired service for the user device with the service provider via the bridging user device and the first wireless network, and through a second wireless network that couples the bridging user device to the service provider, where at least the establishing and the recording "use trusted software comprising a certified unit of code running on the user device and on the bridging user device".

Clearly, the amended independent claims are neither anticipated or rendered obvious or unpatentable by the references that have been cited and applied by the Examiner.

The indicated allowability of the claims for this one reason alone should not be construed as an acknowledgment that the Applicant is in agreement with the Examiner's other reasons for

S.N.: 10/792,181  
Art Unit: 2681

rejecting the claims based variously on Tamaki et al. and the other cited documents.

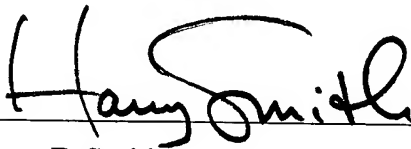
As but one example, dependent claim 21, as amended, recites:

**"where said computer code that establishes said service provisioning relationship includes computer code for negotiating specifics of charging for said trusted service provisioning relationship between said user device and said bridging user device using an offer-counteroffer technique" (emphasis added).**

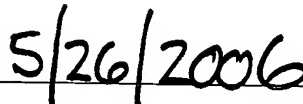
Paragraphs [0031-0033] and [0035] of Tamaki et al. have been carefully reviewed, and no suggestion of the claimed subject matter is found.

The Examiner is respectfully requested to enter the proposed clarifying amendment, to reconsider and remove the rejections of the claims, and to allow all of the pending claims 1-44 as now presented for examination. An early notification of the allowability of claims 1-44 is earnestly solicited.

Respectfully submitted:



Harry F. Smith



Date

Reg. No.: 32,493

Customer No.: 29683

HARRINGTON & SMITH, LLP

4 Research Drive

Shelton, CT 06484-6212

Telephone: (203)925-9400

Facsimile: (203)944-0245

email: hsmith@hspatent.com

S.N.: 10/792,181  
Art Unit: 2681



### CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

5/26/06  
Date

Claine F. Mian  
Name of Person Making Deposit

# trusted software

---

**trusted software:** [The] software portion of a trusted computing base (TCB). [INFOSEC-99]

---

This HTML version of Telecom Glossary 2K was last generated on Wed Feb 28 15:39:21 MST 2001. References can be found in the Foreword.

---

# trusted computing base (TCB)

---

**trusted computing base (TCB):** [The] totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. [INFOSEC-99] *Note:* The ability of a trusted computing base to enforce correctly a unified security policy depends on the correctness of the mechanisms within the trusted computing base, the protection of those mechanisms to ensure their correctness, and the correct input of parameters related to the security policy. [NIS]

---

This HTML version of Telecom Glossary 2K was last generated on Wed Feb 28 15:39:21 MST 2001. References can be found in the Foreword.

---